UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/659,335	09/11/2003	Ikuo Makita	1538.1040	3760

21171 7590 08/20/2008

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/659,335	MAKITA, IKUO	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 12-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/13/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to Response to Restriction/Election filed on April 18, 2008 and to amendment after non-final rejection filed on January 4, 2008.

2. Applicant's election without traverse of Group I (Claims 1-10 and 12-33) in the reply filed on April 18, 2008 is acknowledged.

3. Thus claims 1-10 and 12-33 are pending/examined.

Priority

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

Claim Objections

5. The abstract of the disclosure is objected to because of the following informalities: The description written on lines 10-16 of the abstract does not contain a well defined meaning. For instance the abstract on page 10-16 recites the following "... if it is judged that the first and second digital signatures are not identical, generating first hash data from the first digital signature; comparing the first hash data with second hash data, which is registered in the data storage unit so as to correspond to the specific data; a**nd if it is judged that the first and second digital signatures are identical, granting the user an authority to read the specific data."**

Examiner asserts the above recitation should/could have been written as "... if it is judged that the first and second digital signatures are not

identical, generating first hash data from the first digital signature; comparing the first hash data with second hash data, which is registered in the data storage unit so as to correspond to the specific data; **and if it is judged that the first and second hash data are identical, granting the user an authority to read the specific data."**

Appropriate correction is required. See MPEP § 608.01(b).

Note: This is just one way of correcting the abstract. However applicant's representative could correct the abstract in various ways.

Response to Arguments

6. Applicant's remark/arguments filed on January 4, 2008 have been fully considered but they are not persuasive.

Referring to the independent claims 5, 12, 18, 28 and the pervious independent claim 11, which is not elected by the election, applicant's representative argued and wrote the following.

"Independent claims 5, 12, 18, 28 do not recite the feature "receiving a first digital signature for specific data stored in said center system and a request to allow a first user to read said stored specific data, from a terminal of a second user." Accordingly, Applicants respectfully submit that the rejection of claims 5, 11, 12, 18 and 28 appears to be in error. Accordingly, Applicants respectfully request a new, non-final Office Action, if necessary, addressing the features of each and every claim, for example, the claim features "if specific data is received by said center system from a user terminal, generating hash data for said specific data;

transmitting said hash data to said user terminal; receiving a digital signature generated from said hash data from said user terminal; and registering said specific data, said hash data and said digital signature into a data storage unit, wherein the registered hash data and the registered digital signature are used to confirm if an authority to access said specific data is granted to an access requestor" **as recited, for example, in claim 11."**

Examiner disagrees with the above argument.

Examiner would point out that the limitation that is argued above is recited in claim 11 which is found be distinct from the rest of the claims and claim 11 was restricted in the office action set forth previously. Furthermore applicant's representative did not elect this claim thus the above argument is no more applicable after the election is made.

The rest of the independent claims are drawn to an information processing method/an access method/executed by a center system, said information processing method comprising: receiving a first digital signature for specific data stored in said center system and a request to allow a first user to read/update said stored specific data, from a terminal of a second user; confirming if an authority to give said first user permission to read/update said stored specific data is granted to said second user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; and if said first signature and said second signature are identical, performing a processing for enabling **said first user to read/update said stored specific data.**

And examiner would point out that such limitation is disclosed by the combination of the reference/s on the record.

For instance

Referring to the respective independent claims 1, 5, 12, 14, 18, 24 and 28 Bowe, the primary reference on the record, discloses information processing method executed by a center system *[See at least Paragraph 0054, "a server-side digital signature system/method],* **said information processing method comprising:**

receiving a first digital signature for specific data stored in said center system and a request to allow a first user to be allowed to read said stored specific data, from a terminal of a second user *[See abstract and figure 3, paragraph 0060] (On abstract the following has been disclosed. "A digital signature system is provided on a server for use by remote clients, such as by using a browser. The server generates and maintains all of the users' keys used for producing a digital signature. A user sends a data object to the server, and the server generates a digital signature for the data object using the private key stored at the server. The server then sends the digital signature to the client.* ***A client can, at a later time, send the signature back to the server for verification.****" Furthermore on paragraph 0060 and figure 3, the following has been disclosed/shown. "FIG. 3 shows a Verification Request and a Verification Response according to the present invention. Client 100 can later send the signed object 230 to the server 120 for verification. The server verifies the signature by obtaining the data object 210 and the hash from the first*

signature 225 from the signed object. ***The server generates a second hash 310 using the data object and compares the hash from the first signature 225 with the second hash 310. If the signatures match, the signature is valid.*** *The server returns an indicator 320 showing the status of the signature, either valid or invalid.")*

And;

comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; [paragraph 0060 and figure 3] (On paragraph 0060, the following has been disclosed. *"FIG. 3 shows a Verification Request and a Verification Response according to the present invention. Client 100 can later send the signed object 230 to the server 120 for verification. The server verifies the signature by obtaining the data object 210 and the hash from the first signature 225 from the signed object. The server generates a second hash 310 using the data object and compares the hash from the first signature 225 with the second hash 310.* ***If the signatures match, the signature is valid****. The server returns an indicator 320 showing the status of the signature, either valid or invalid.")* and

Furthermore on figure 3, **Bowe discloses that** if first signature and said second signature are identical, sending a verification Response & indicator.

Bowe, the primary reference on the record, does not explicitly disclose

- **Confirming if an authority to give said first user permission to read/update data by comparing the received first digital signatures with second digital signature.**

However, in the same field of endeavor, Spain discloses the following, which meets the above limitation,

"A digital signature generator is included to create a digital signature of the hardware address of the hardware element. A memory element stores the digital signature of the hardware element. A software program is included to compare the digital signature of the hardware element to a known value. **If the digital signature of the hardware element matches the known value, the user may be granted read and write/update access to all memory locations within the memory element**, including a location in which the hardware address is stored." [See at least the abstract]

The next argument presented by the applicant's representative is referring to the independent claims.

Applicant's representative in particular argued that assertion that the examiner made referring to Spain, the secondary reference on the record, disclosing the limitation recited as "**Confirming if an authority to give said first user permission to read/update data by comparing the received first digital signatures with second digital signature**" is incorrect , because applicant's argued that although Spain discloses, "comparing the digital signature of the hardware element to a known

value," as recited in claim 1 of Spain, as asserted by the Examiner, the digital signature in Spain is decrypted before being compared with the "known value" (see, for example, Spain at steps 440-460 of FIG. 4).

Examiner disagrees.

Examiner would like to point out that the limitation recited in each independent claim does not specific the fact that the digital signature should be compared with out being decrypted. Besides the secondary reference on the record namely Spain, on the abstract, discloses the following which meets the above argued limitation. "A digital signature generator is included to create a digital signature of the hardware address of the hardware element. A memory element stores the digital signature of the hardware element. A software program is included **to compare the digital signature of the hardware element to a known value. If the digital signature of the hardware element matches the known value, the user may be granted read and write access to all memory locations within the memory element, including a location in which the hardware address is stored.**" [Abstract]

Thus even on the abstract, as shown above, Spain does not specify that the digital signature is decrypted before it is compared because such specific is not found to be relevant and the bottom line is the user is allowed to read/write/update based on the authenticity or based on the comparison of the digital signature. Thus whether or not the digital signature is decrypted before it is compared is an obvious variation for one of ordinary skill in the art.

Lastly applicant's representative argued that a prima facie case of obviousness cannot be based upon Bowe and Spain, because there is no evidence that one skilled in the art would have been led to combine Bowe and Spain and modify the combination to include the claimed limitation recited in the respective independent claims

Examiner disagrees with the above argument.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). **In this case, the two reference/s are combined** because it would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of comparing digital signatures before granting access for read/write as per teachings **Spain** into the method as taught by **Bowe** in order to **verify the authenticity of the request before granting access to read/write. [See Spain, lines 58-59]**

Thus the rejection is maintained until the applicant's successfully overcome the ground of the rejection set forth in present office action.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1-10 and 12-33** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Bowe et al** (hereinafter referred as **Bowe**) (U.S. Publication No. 2003/0093678 A1) (filed on April 23, 2001) in view of Spain et al (hereinafter referred to as **Spain**) (U.S. Patent No. 7,058,811 B2) (filed on 10/31/2001)

9. **As per independent claims 1, 5, 12, 14, 18, 24 and 28 and dependent claims 29-33 Bowe discloses an information processing method executed by a center system** *[See at least Paragraph 0054, "a server-side digital signature system/method],* **said information processing method comprising:**

receiving a first digital signature for specific data stored in said center system and a request to allow a first user to be allowed to read said stored specific data, from a terminal of a second user *[See abstract and figure 3, paragraph 0060] (On abstract the following has been disclosed. "A digital signature system is provided on a server for use by remote clients, such as by using a browser. The server generates and maintains all of the users' keys used for producing a digital signature. A*

user sends a data object to the server, and the server generates a digital signature for the data object using the private key stored at the server. The server then sends the digital signature to the client. ***A client can, at a later time, send the signature back to the server for verification.*** *" Furthermore on paragraph 0060 and figure 3, the following has been disclosed/shown. "FIG. 3 shows a Verification Request and a Verification Response according to the present invention. Client 100 can later send the signed object 230 to the server 120 for verification. The server verifies the signature by obtaining the data object 210 and the hash from the first signature 225 from the signed object.* ***The server generates a second hash 310 using the data object and compares the hash from the first signature 225 with the second hash 310. If the signatures match, the signature is valid.*** *The server returns an indicator 320 showing the status of the signature, either valid or invalid.")*

And;

comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said stored specific data; [paragraph 0060 and figure 3] (On paragraph 0060, the following has been disclosed. *"FIG. 3 shows a Verification Request and a Verification Response according to the present invention. Client 100 can later send the signed object 230 to the server 120 for verification. The server verifies the signature by obtaining the data object 210 and the hash from the first signature 225 from the signed object. The server generates a second hash 310 using the data object and*

compares the hash from the first signature 225 with the second hash 310. ***If the signatures match, the signature is valid****. The server returns an indicator 320 showing the status of the signature, either valid or invalid.")*

and

Furthermore on figure 3, **Bowe discloses that** if first signature and said second signature are identical, sending a verification Response & indicator.

Bowe does not explicitly disclose

- Confirming if an authority to give said first user permission to read data by comparing the received first digital signatures with second digital signature.

However, in the same field of endeavor, Spain discloses the following, which meets the above limitation,

"A digital signature generator is included to create a digital signature of the hardware address of the hardware element. A memory element stores the digital signature of the hardware element. A software program is included to compare the digital signature of the hardware element to a known value. **If the digital signature of the hardware element matches the known value, the user may be granted read and write access to all memory locations within the memory element**, including a location in which the hardware address is stored." [See at least the abstract]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of comparing

digital signatures before granting access for read/write as per teachings **Spain** into the method as taught by **Bowe** in order to **verify the authenticity of the request before granting access to read/write. [See Spain, lines 58-59]**

10. **As per claims 2, 15 and 25 the combination of Bowe and Spain discloses an information processing method as applied to claims above. Furthermore Bowe discloses the method, wherein said performing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, and which represents that an authority to read said specific data is granted to said first user, to a terminal of said first user.** *[Paragraph 0060 and figure 3] (On paragraph 0060, the following has been disclosed. "FIG. 3 shows a Verification Request and a Verification Response according to the present invention. Client 100 can later send the signed object 230 to the server 120 for verification. The server verifies the signature by obtaining the data object 210 and the hash from the first signature 225 from the signed object. The server generates a second hash 310 using the data object and* ***compares the hash from the first signature 225 with the second hash 310. If the signatures match, the signature is valid. The server r****eturns an indicator 320 showing the status of the signature, either valid or invalid.")*

11. **As per claims 3-4,6-10, 13, 16-17,19-23 and 26-27 the combination of Bowe and spain discloses an information processing method as applied to claims above. Furthermore Bowe discloses the method,**

further comprising: said first signature and said second signature are not identical, generating second hash data from said first digital signature; confirming if said authority to give said first user first user said permission to read specific data is granted by said second user by comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said specific data; and executing a processing for enabling said first user to read said specific data. [See at least paragraph 0036] *(On paragraph 0036, Bowe discloses the following . "Subsequently, upon a request from the client, the server authenticates the signed object by deriving the original data object and the signature from information obtained from the signed object sent by the client. The server then generates a comparison value by hashing the original data object to produce a second hash, and comparing the hash value in the signature to the second hash. The server also checks the hash value in the signature using the user's public key. If the document is authenticated, the server notifies the client that the authentication was successful." Furthermore, Spain on the abstract discloses the following. "A digital signature generator is included to create a digital signature of the hardware address of the hardware element. A memory element stores the digital signature of the hardware element. A software program is included to compare the digital signature of the hardware element to a known value. If the digital signature of the* ***hardware element matches the known value, the user may be granted read and write access to all memory locations***

within the memory element, including a location in which the hardware address is stored.")

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(PTO-Form 892).

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

08/10/2008
/Samson B Lemma/
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132